

Applicant's Interview Summary Record

Applicant thanks Examiner Abrishamkar for his time and attention during the 10/23/07 personal interview. That interview was attended by:

- inventor Timothy Simms,
- Joel Haspel (representative of assignee company Plethora Technology),
and
- representative Rob Faris.

During the interview, Mr. Haspel gave Examiner Abrishamkar background concerning Plethora Technology. He explained that Plethora is an eight-person company based in Charles Town West Virginia with primarily a Federal Government customer base (e.g., Dept. of Labor, Dept. of Energy, Dept. of Transportation). Mr. Haspel explained that Plethora's current business is directed to providing remote connectivity for users who wish to access their desktop remotely. He said that one of Plethora's current products is a USB stick marketed as "Enterprise In a Flash" that contains authentication software and other information allowing a user to securely, remotely connect to an enterprise server from a variety of different types of remote personal computers with different processing capabilities.

Mr. Haspel and Mr. Simms explained that the exemplary illustrative non-limiting implementation of Plethora's technology as deployed in the commercial marketplace is able to remote a user's desktop using strong security without any need to disclose passwords or keys over the network, in a way that is not susceptible to eavesdropping or other "man in the middle" attacks and to provide protection against replay attacks.

Mr. Haspel characterized the exemplary illustrative non-limiting implementation of Plethora's technology in the commercial marketplace as elegant, minimalistic and fast.

Mr. Haspel explained that Plethora's commercial product includes so-called "single ended authentication" with powerful encryption and the ability to establish a secure authenticated session with relatively low overhead. Mr. Haspel explained that such feature is ever more important as users go into uncontrolled environments where they nevertheless need to establish such a secure session with relatively low overhead to thereby provide rapid, secure remote connectivity.

Mr. Simms explained that he initially set out to build a secure channel "from the ground up" in order to provide better performance and faster speed. Mr. Simms explained that certain prior art arrangements required both ends (i.e., server and client) to generate, with relatively high overhead, sessions keys such as public key encryption pairs. Mr. Simms explained that his objective in developing the exemplary illustrative non-limiting implementation disclosed this patent application was to establish the same shared session key on both sides (e.g., server and client) without high overhead on the client side. He explained that this can be important given that the client might be a relatively low-capability device not capable of processing very rapidly.

Mr. Haspel mentioned IPsec and SSL as examples of secure, known security protocols that he characterized as being relatively "bloated" in the sense that they are relatively computationally intensive and require the remote client to do a lot of processing. Mr. Simms explained that he set out to streamline the secure session protocol so that a remote device could establish a secure session as quickly as possible even if it could not process very fast. Mr. Haspel explained the desirability of providing

portability without the need to install software in advance and without the need for fast hardware.

Mr. Haspel and Mr. Simms explained the desirability of a user side experience that allows for example a USB stick to be plugged into a remote computer to allow fast, secure remote login. Mr. Haspel explained that while there are various commercially available secure virtual private networks (VPN) and the like, using IPSec or other protocols and technologies, they often or sometimes can take many seconds or sometimes even minutes to establish a secure session.

Mr. Simms explained in detail how the exemplary illustrative non-limiting implementation described in the subject patent application establishes a secure session. Mr. Haspel drew a diagram for the Examiner explaining the back and forth protocol disclosed in the exemplary illustrative non-limiting implementation of the subject application. Some discussion focused around the use of a password to encode information exchanged over the network. Mr. Simms explained that the password could be used to "encrypt" but could also be used to provide other forms of encoding such as through use of a one-way hash function.

Examiner Abrishamkar thanked the applicant for attending the interview. He said that he now had a good understanding of Plethora's technology and he indicated that it was likely he would conclude that amended claims would distinguish over the applied references. The Examiner indicated that he would need to conduct a further search and also consult an even more experienced Examiner in the USPTO specializing in encryption-based protocols. Mr. Abrishamkar indicated that he would carefully consider any further amendment and advise the applicant by telephone if further claim

amendments seemed to be necessary or helpful to obtain allowance. Mr. Faris invited the Examiner to call him to discuss any remaining issues that might potentially stand in the way of allowance, and said that the applicant would be filing a response shortly. The present filing constitutes that response.